AMENDMENTS TO THE CLAIMS

Claims 1 through 16 (Canceled)

17. (Currently Amended) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by a third party, a hard copy transaction certificate with an encrypted code ~~by a third party~~;

scanning the received transaction certificate to convert the encrypted code into electronic form;

retrieving a public key of the first party;

decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring the conducted transaction ~~between a first party and a second party~~ including the decrypted proof elements as authenticated by the third party if the decrypting is successful.

18. (Currently Amended) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by a third party, a transaction certificate with an encrypted code;

retrieving a public key of the first party;

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring the conducted transaction ~~between a first party and a second party~~ including the decrypted proof elements as authenticated if the decrypting is successful.

19. (Currently Amended) A method of a third party authenticating a transaction conducted between a first party and a second party, the method comprising:

receiving, by the third party, an encrypted transaction certificate;

decrypting the received encrypted transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code;

retrieving a public key of the first party;

decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

declaring, by the third party, the transaction including the decrypted proof elements as authenticated if the decrypting is successful.

20. (Canceled)

21. (Currently Amended) A computing device for verifying, by a third party, a transaction conducted between a first party and a second party, the device comprising:

a receiving module configured to receive a transaction certificate with an encrypted code~~elements of the transaction from the second party~~;

a retrieving module configured to retrieve a public key of a first party; and

a decrypting module configured to decrypt the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

a declaring module configured to declare, on behalf of the third party, the transaction including the decrypted proof elements as authenticated if the decrypting is successful.

~~a first encryption module configured to identify at least a portion of the received transaction elements as selected elements, to encrypt the selected elements based on a private key of the first party to generate an encrypted code, and to attach the encrypted code and at least a portion of the received transaction elements to a transaction certificate;~~

~~a second encryption module configured to encrypt the transaction certificate based on a public key of the second party to generate an encrypted transaction certificate; and~~

~~a transmission module configured to transmit the encrypted transaction certificate from the first party to the second party,~~

~~wherein the encrypted transaction certificate is decrypted by the second party based on a private key of the second party to generate a decrypted transaction certificate with the encrypted code, wherein the encrypted code is decrypted based on a public key of the first party to generate decrypted selected elements, and wherein the decrypted selected elements are used to prove the transaction.~~

22. (Currently Amended) A computing device for verifying, by a third party, a transaction conducted between a first party and a second party, the device comprising:

~~a submitting module configured to submit transaction elements of the transaction from the second party to the first party;~~

a receiving module configured to receive a hard copy transaction certificate including an encrypted code ~~from the first party to the second party~~;

a scanning module configured to scan the received hard copy transaction certificate into electronic form;

a retrieving module configured to retrieve a public key of the first party;

a decrypting module configured to decrypt the scanned encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

a declaring module configured to declare, on behalf of the third party, the transaction including the decrypted proof elements as authenticated if the decrypting is successful.

~~a first decryption module configured to decrypt the encrypted code to generate decrypted proof elements, based on a public key of the first party,~~

~~wherein the decrypted proof elements are used to prove the transaction.~~

23. (Currently Amended) A computing device for verifying, by a third party, a transaction conducted between a first party and a second party, the device comprising:

a receiving module configured to receive an encrypted transaction certificate;

a retrieving module configured to retrieve a public key of the first party;

a decrypting module configured to decrypt the received encrypted transaction certificate based on a private key of the third party so as to generate a transaction certificate with an encrypted code, and further configured to decrypt the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements; and

a declaring module configured to declare, on behalf of the third party, the transaction including the decrypted proof elements as authenticated if the decrypting is successful.

~~a submitting module configured to submit transaction elements of the transaction from the second party to the first party;~~

~~a receiving module configured to receive an encrypted transaction certificate from the first party to the second party;~~

~~a first decryption module configured to decrypt the received encrypted transaction certificate, based on a private key of the second party, to generate an decrypted transaction certificate with an encrypted code; and~~

~~a second decryption module configured to decrypt the encrypted code based on a public key of the first party to generate decrypted proof elements,~~

~~wherein the decrypted proof elements are used to prove the transaction.~~

24. (New) The method of Claim 18, wherein receiving the transaction certificate comprises receiving an e-mail containing the transaction certificate.

25. (New) The method of Claim 18, wherein receiving the transaction certificate comprises receiving an e-mail containing a URL of the transaction certificate.

26. (New) The method of Claim 24, wherein the e-mail is sent by the first party.

27. (New) The method of Claim 24, wherein the e-mail is sent by the second party.

28. (New) The method of Claim 21, wherein the receiving module receives the transaction certificate comprises in an e-mail containing the transaction certificate.

29. (New) The method of Claim 21, wherein the receiving module receives the transaction certificate comprises in a URL containing the transaction certificate.

30. (New) The method of Claim 28, wherein the e-mail is sent by the first party.

31. (New) The method of Claim 28, wherein the e-mail is sent by the second party.